PROCEDURES FOR DATA RELEASE

A. INTRODUCTION

Chapter 43.371 RCW directs the Office of Financial Management (OFM) to establish and adopt rules for a statewide All Payer Claims Database (WA-APCD). Specifically, OFM has statutory authority to enact rules on the following topics:

- Procedures for data release (RCW 43.371.070(1)(g)
- Procedures for ensuring compliance with state and federal privacy laws (RCW 43.371.070(1)(e)

Paper 5 provides background information to inform the development of these rules. In addition, this paper focuses specifically on procedures for ensuring privacy and security in data release, part of the procedures for ensuring compliance with state and federal privacy laws.

For this paper OFM reviewed:

- Data release provisions in other state APCD statutes, rules, policies and procedures.
- Data release documents in other states, including data request forms, data management plans, data use agreements, confidentiality agreements and institutional review board (IRB) approvals.
- Centers for Medicare & Medicaid Services (CMS) Data Management Plan Guidelines and Data Management Plan Evaluation Guide.
- Federal and state privacy laws.
- WA-APCD data release provisions in Chapter 43.371 RCW.
- Washington State's Office of the Chief Information Officer Policy 141 Securing Information Technology Assets Standards.
- Competitive Procurement #16-100 APCD Appendix B Sample Contract, Sections 16–20.
- Washington Health Alliance All Payer Claims Database Data Release Advisory Committee Summary of Recommendations.[1]

Paper 5 is divided into the following sections:

1. OFM contracted with the Washington Health Alliance to convene a Data Release Work Group to provide technical advice on data release requirements for the WA-APCD. OFM submitted the final report as a deliverable for the Centers for Medicare & Medicaid Services, Center for Consumer Information and Insurance Oversight, Health Insurance Rate Review Grant Program, Cycle III grant that OFM received in October 2013. For the full report, see the OFM Health Transparency website at: http://www.ofm.wa.gov/healthcare/pricetransparency/pdf/data_release_recommendations.pdf.

Appendices and References

B. OVERVIEW OF DATA RELEASE IN OTHER STATES

OFM reviewed data release in seven states with established APCDs — Colorado, Maine, Maryland, Massachusetts, New Hampshire, Oregon and Vermont.

The states release APCD data for public and private purposes that are specified in their APCD statutes or rules. The *public* purpose for data release is to provide consumers free access to health care data on the APCD website. The public data include information on some or all of the following health care topics: performance, quality, health outcomes, health disparities, utilization and pricing. Some APCD websites include documentation that describes the essential features of the reports such as the underlying data and the methodologies used to analyze the data. The *private* purpose for data release is to provide data to requesters for specific uses such as health care studies, comparative analyses or specialized reports. The states charge fees for the release of the private data.

The states authorize access to different levels of data.[2] The most common levels of data access include:

- **De-identified data sets**. The data do not directly or indirectly identify individuals. States often refer to de-identified data sets as public use data sets.
- **Limited data sets**. The data contain some protected health information data elements but exclude a list of direct patient identifiers or identifiers of relatives, employers or household members of the patient.
- **Identifiable data sets**. The data contain direct patient identifiers — name, Social Security number, date of birth, etc. — that uniquely identify an individual or can be combined with other readily available information to uniquely identify an individual. Identifiable data sets are typically released for approved research purposes.

In addition to the three levels of data access mentioned above, Colorado authorizes custom reports that can be requested for release. Custom reports contain a summary or analyses of data derived from the Colorado APCD database such as counts, totals, rates per thousand, index values and other standardized metrics. A custom report never displays claims lines or member-level detail.

2. See Appendix B Data access in other states.

Vermont authorizes access to two data sets — a public use data set that contains unrestricted data elements and a limited use health care research data set that contains restricted data elements and is released only for research purposes.[3]

Some states authorize data release to different types of data users such as government agencies, private entities or researchers. Other states do not identify different types of data users.

Most of the states have roles and responsibilities for the APCD administrator and a data review committee (DRC) in the data release process.[4] APCD administrator responsibilities typically are to:

- Maintain a list of data elements for each level of data release.
- Receive and review the data requests for completeness.
- Determine if a data request requires a DRC review.
- Appoint the DRC members. In some states, DRC membership is specified in the APCD statutes. Some APCD administrators add technical experts to the DRC.
- Provide support to the DRC for meeting schedules, agendas, facilitation and minutes.
- Make the final decisions to approve or deny data requests.
- Notify the data requesters about the final decisions on their data requests.
- Post the approved data requests on the APCD website.[5]
- Collect the fees for the data.
- Authorize the data release.
- Provide updates and reports as needed.
- Ensure that data are destroyed or returned at the end of projects.

The DRC is responsible for reviewing the data requests and making a recommendation to the APCD administrator to release or not to release the data. The DRC may obtain assistance from outside entities, such as privacy and security experts, to help with the data request review.

3. List of the unrestricted data elements in Vermont's public use data set and the restricted data elements in the limited use health care research data set are found in Vermont Regulation H-2008-01 Vermont Healthcare Claims Uniform Reporting and Evaluation System, Appendix J-2 Data Release Schedule http://www.dfr.vermont.gov/sites/default/files/REG-H-08-01.pdf.
4. The DRC is appointed by the APCD administrator based on membership requirements listed the state APCD statute or rule. The DRC has different names in each state. Colorado calls it the Data Release Review Committee. Maine calls it the Data Release Subcommittee. Massachusetts calls it the Data Release Committee. Oregon calls it the Data Review Committee. New Hampshire calls it the Claims Data Release Advisory Committee. Vermont calls it the Data Release Advisory Committee.
5. In Maryland, the Staff Review Committee (SRC) reviews application for the qualifications of the applicant, whether the data request is appropriate for the research goals and whether the data security standards are met. The SRC may recommend approval to the Maryland Health Care Commission. The commissioners review all data request applications and have the ultimate authority to approve release of the data.

The states follow the same basic steps for the data release process. The steps are:

1. **Data requester prepares a data request.**
   The data requester reviews the APCD data dictionary[6] to determine the data needed for the project(s). Often APCD staff help the data requester identify the best ways to:
   - Tailor the data request.
   - Understand state privacy and security requirements.
   - Understand uses and limitations of the data products.
   - Calculate fees for the data.

2. **Data requester submits a written data request to the APCD administrator.**
   The data requester has to submit a written data request that includes the following documents:
   - Data request form. The data request form includes detailed information about the project. This form must be signed by the data requester and, if applicable, representatives from any third-party organizations that will have access to the data during the course of the project. For more details about data request forms, see Appendix C Data request forms in other states.
   - Data management plan (DMP). A data management plan is a formal document that outlines how a data requester will handle the APCD data to ensure privacy and security both during and after the project. For more details about DMPs, see Appendix D data management plans in other states.
   - Data use agreement (DUA). The data use agreement is a legally binding document signed by the APCD administrator and the data requester that defines the terms and conditions under which the state allows access to and use of the APCD data and how the data will be secured and protected. Some states have one DUA for all data requesters. Other states have more than one DUA, depending on the entity applying for data release. For example, Massachusetts has a DUA for government agencies and a DUA for nongovernmental entities. Massachusetts also has addendums to the DUA for Medicare and MassHealth data (Medicaid).[7] Oregon has one DUA for public use files and another DUA for other data release. For more details on DUAs, see Appendix E data use agreements in other states.
   - Confidentiality agreement. In some states, signed confidentiality agreements are required in addition to a DUA. In other states, the confidentiality provisions are included in the DUA. For more details on confidentiality agreements, see Appendix F confidentiality statement.
   - Copies of the privacy and security policies of the data requester's organization and any third-party organizations that are listed on the data request form.

6. A data dictionary is a set of information describing the contents, format and structure of a database, and the relationship between its elements, used to control access to and manipulation of the database.
7. Many of the provisions are the same in the Medicare and MassHealth addendums to the DUA. One difference is that the cell size suppression policy for CMS data states that no cell fewer than 10 (admittances, discharges, patients, services) may be displayed. On the other hand, the cell size suppression policy for Massachusetts APCD states that no fewer than 11 (admittances, discharges, patients, services) may be displayed.

- Copy of an institutional review board (IRB) approval. An IRB is a committee that is established to review and approve research involving human subjects to ensure the research is conducted according to federal and state privacy laws and ethical guidelines. IRB approval is typically required for research projects that request direct patient identifiers.[8]

The data requesters submit the completed and signed documents to the APCD administrators.

3. Review the data request.

The APCD staff conduct an initial review to determine if the applications are complete and that the research requests for identifiable data include an IRB approval letter, if required.

Requests for limited data sets and identifiable data sets require a DRC review to ensure that the data are being used properly and there are adequate privacy and security provisions in the DMP to protect the data both during and after the project. The DRC also checks that data requesters:

- Do not request more data than is necessary to complete their projects.
- Agree to adhere to the minimum cell size policy (usually no fewer than 11 elements per cell) and use complementary cell suppression techniques when working with small numbers.[9]
- Agree not to link or combine data or information from other sources to identify individuals.
- Agree to aggregate data in reports or products to protect individuals from being identified.

The DRC makes recommendations to the APCD administrator to approve or deny data requests.

In Oregon, the APCD administrator posts data requests on the website for public input two weeks before the DRC is scheduled to review the requests. The public input is considered as part of the DRC review.

In Maine, the APCD administrator adds new data requests to the website weekly. The Web information includes the identities and addresses of all parties requesting data, the level of data requested and the purpose of the request. The APCD administrator also notifies data providers and other interested parties of new data requests. Notice of the Level III data requests is published in at least three major news publications.

For all data requests, the data providers or other interested parties may submit comments related to the data request no later than 30 business days after the initial posting of the data

8. For a good overview of IRBs, see James Bell Associates (2008). Evaluation Brief: Understanding the IRB. Arlington, V.A. January 2008 http://betterevaluation.org/sites/default/files/understanding%20the%20irb.pdf. There are public and private IRBs. Some states designate an IRB to review their APCD data requests. For example, Maryland designated a private IRB, Chesapeake IRB, for reviews of research data requests before they are reviewed by the Maryland Health Care Commission.
9. Cell size suppression is a statistical method used to report aggregate data in tables that restrict or suppress disclosure of subsets of aggregate data to protect the identity and privacy of data subjects and to avoid the risk of identification of individuals in small population groups.

request on the Maine website. If the APCD administrator determines that (a) the comments received are of significant enough importance to delay the release of data and/or (b) additional information is required from the requesting party to address the comments, then the data will not be released until the additional information has been received from the requesting party and an additional review is conducted by the APCD administrator or data release subcommittee.

4. **Approve or deny the data request.**

The APCD administrator receives one of the following recommendations from the DRC:

- Approve the data request.
- Conditionally approve the data request pending receipt of additional information.
- Deny a data request.

The APCD administrator considers comments from the staff, the DRC recommendation and, in some states, public input on data requests before approving the data requests.

APCD administrators can deny a data request. Oregon APCD rules authorize denial of a data request for reasons which include, but are not limited to:

- The requester has previously violated a data use agreement.
- Proposed purpose for accessing the data is not allowable under policies or state or federal rules, regulations or statutes.
- Any person who will have access to the data has previously violated a data use agreement.
- Full payment is not included with the application.
- The proposed privacy and security protections are not sufficient.
- Information provided is not sufficient to approve the request.

In most of the states, the APCD rules do not list specific reasons for the APCD administrator to deny a data request.

If the APCD administrator denies a data request, the states allow the data requester to appeal.

After finalizing the decisions on the data requests, APCD administrators publish a summary of the approved data requests on their APCD websites.

5. **Release the data.**

The APCD administrator sends a notice of approval to the data requester.

States require that the fees be paid before the data is released. Fees may include application fees, consulting fees to provide APCD staff with assistance in preparing the data request and fees for the data extract. In some states, the APCD administrator calculates the fees for the data request and informs the data requester of the total cost. In Oregon, the data requester can calculate the total cost of standard limited data sets on the electronic data request form and submit a check with the data request.[10]

10. See page 13 of Form APAC-3 http://www.oregon.gov/oha/OHPR/RSCH/Documents/APAC-3_Application.pdf.

The data extract is prepared by the APCD data aggregator and sent to the data requester in an encrypted and secure manner.

6. **Destroy or return data at the end of the project.**
   The data recipient must present proof that the data are destroyed or returned at the end of the project(s.) Some states have a certificate that must be completed and returned to the APCD administrator to certify that the data have actually been destroyed or retained at the end of the DUA.[11]

   If a data recipient's project extends longer than the term of the DUA, the APCD administer may renew or renegotiate the DUA with the data recipient.

   Some of the state rules or data use agreements include timelines for each step in the data release process. See Appendix H Timelines for the data release process in other states.

C. PRIVACY AND SECURITY PROCEDURES FOR DATA RELEASE IN OTHER STATES

Before releasing data, APCD administrators have to ensure there are organizational, personnel/staffing and technical safeguards to ensure privacy and security in the recipients' data environments. APCD administrators rely on good data management plans and enforceable data use agreements to do this.

For taking possession of and storing the data files, the data recipients and subcontractor(s) should have the following organizational, technical and personnel/staffing safeguards in place:

- A list of the contact information for the individual(s) responsible for organizing, storing and archiving data.
- A list of all agreements that bind the organization and individuals to the privacy and security rules for using the data files. Agreements include nondisclosure agreements, rules of behavior, memoranda of understanding, confidentiality agreements, subcontracts, etc.
- A current inventory of the files received and a plan to inventory new files received.
- Explanation of the infrastructure (facilities, hardware, software, etc.) that will be used to store the APCD data files.
- Written policies for the physical possession and storage of the APCD data files.
- Adequate physical security of all premises where data sets are stored or processed.
- A process to track the status and roles of the individuals on the research team, e.g., researcher with full access, researcher with limited access, etc.
- A process to inform the APCD administrator of any staff changes on the project and name of the contact person who will notify the APCD administrator.
- A list of all security and privacy trainings that the project staff are required to take.
- Reasonable precautions with respect to the employment of personnel who could have access to data sets, e.g., background checks, reference checks.

11. See Appendix B: Colorado's certificate of project completion and data destruction or retention.

For data sharing/electronic transmission, the data recipients and subcontractors should have the following organizational, technical and personnel/staffing safeguards in place:

- Written policies and procedures for physical removal, transport and transmission of APCD data, including if data are in a different location. For example:
  - Do not allow data provided by the APCD administrator to be physically moved or electronically transmitted unless written authorization is received from the APCD administrator.
  - Do not allow any data provided by the APCD administrator to be physically moved or electronically transmitted outside the United States.
  - Do not disclose any patient-specific information to any person or entity outside of the parties stated in the DUA.
  - Name of organization(s) that will share the data and a contact person's information.
- Guidelines for transmitting and receiving data. For example, Oregon's All Payer All Claims (APAC) database guidelines for receiving data state that:
  - APAC sets will be encrypted and sent in pipe-delimited text files over secure FTP.
  - APAC data sets range in size from 6 GB to 46 GB. For example, one year of pharmacy data will comprise more than 30 million rows, whereas one year of all medical claims will comprise more than 100 million rows.
  - Recommended software for importing/analyzing APAC data sets are SAS, SQL and SPSS. APAC data sets are generally too big for Microsoft Excel and Access.
- Maintain all patient-specific information on password-protected computers and in locked offices.
- Implement appropriate authentication credentials.
- Implement technical protocols, including:
  - Passwords with appropriate complexity standards to protect data sets from wrongful access
  - Log-on/log-off
  - Session time out
  - Encryption of data in motion and data at rest
- Test and audit controls.
- Limit access to the data to the minimum number of individuals necessary to achieve the purpose.
- Grant levels of access based on need-to-know only.
- Take reasonable precautions with respect to the employment of and access given to personnel who could have access to data sets.

For data reporting and publication, data recipients and subcontractors should have the following organizational safeguards in place:

- Use only the minimum amount of data needed to accomplish the intended purpose of the data request.
- Have a cell size suppression policy for dealing with small numbers. Cell size means the count of patients who share a set of characteristics contained in a statistical table.

- Include the following common data use restrictions in the DUA:
  - No identification of individuals
  - No re-engineering data
  - No linking data except with permission

For completion of research and data destruction, data recipients and subcontractors should have the following organizational, technical and personnel/staffing safeguards in place:

- Limit the time frame of the DUA. Have the option to renew for longer projects, if needed.
- Have a documented process to complete the certificate of destruction of data according to the APCD administrator's requirements.
- Require proof of data destruction within a fixed time period after the end of the DUA.
- Give APCD administrator authority to audit data recipients, including onsite visits on short notice.
- Have penalties for breach of DUA, including the right of the APCD administrator not to release data again to a noncompliant data recipient.
- Have policies and procedures to ensure original data files are not used following the completion of a project.
- Have policies and procedures to inform the APCD administrator when the staff leave the project voluntarily or involuntarily.

D. CHAPTER 43.371 RCW PROVISIONS FOR WA-APCD DATA RELEASE

Chapter 43.371 RCW includes detailed data release provisions for the WA-APCD.

RCW 43.371.020(1) states the purpose of the WA-APCD is to provide data to support transparent public reporting of health care information to:

- Assist patients, providers and hospitals to make informed choices about care.
- Enable providers, hospitals and communities to improve by benchmarking their performance against that of others by focusing on best practices.
- Enable purchasers to identify value, build expectations into their purchasing strategy and reward improvements over time.
- Promote competition based on quality and cost.

RCW 43.371.020 includes detailed definitions for the claims data and variables that can be released and a definition for a "unique identifier" used to link an individual's data longitudinally. The definitions include the following:

> **"Direct patient identifier**" means a data variable that directly identifies an individual, including names; telephone numbers; fax numbers; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate or license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web universal resource locators; Internet protocol address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

"Indirect patient identifier" means a data variable that may identify an individual when combined with other information.

"Proprietary financial information" means claims data or reports that disclose or would allow the determination of specific terms of contracts, discounts or fixed reimbursement arrangements or other specific reimbursement arrangements between an individual health care facility or health care provider, as those terms are defined in RCW 48.43.005, and a specific payer, or internal fee schedule or other internal pricing mechanism of integrated delivery systems owned by a carrier.

"Unique identifier" means an obfuscated identifier assigned to an individual represented in the database to establish a basis for following the individual longitudinally throughout different payers and encounters in the data without revealing the individual's identity.

RCW 43.371.050(1) authorizes other data from the database to be released. Other data include procedure codes; diagnoses codes; age; gender; claim paid date; billed, allowed and paid amounts (in some circumstances); service date; and provider information. These data are included in health care claims and submitted by the data suppliers. The term "other claims data" is not defined in the WA-APCD statute.

RCW 43.371.050(1) authorizes the release of claims or other data from the database in processed form to public and private requesters.

RCW 43.371.050(4)(a) to (d) authorizes the following data access, depending on the data requester:

- **Researchers with IRB approvals** can request direct patient identifiers, proprietary financial information, indirect patient identifiers, unique identifiers and other data or any combination thereof to the extent the data are necessary to achieve the goals of the WA-APCD. Researchers must use the data release process to request the data and sign data use agreements and confidentiality agreements with the lead organization before the data are released. [12]
- **Federal, state and local government agencies** can request proprietary financial information, indirect patient identifiers, unique identifiers and other data, or any combination thereof, but not direct patient identifiers. Federal, state and local government agencies must use the data release process to request the data and sign a data use agreement with OFM and the lead organization before the data are released.
- **Agencies, researchers and other entities** as approved by the lead organization can request indirect patient identifiers, unique identifiers, or a combination thereof, but not proprietary financial information and direct patient identifiers. The agencies and research and other entities must use the data release process to request the data and sign a data use agreement with the lead organization before the data are released.

12. For more information on Washington IRB, see https://www.dshs.wa.gov/sesa/human-research-review-section/frequently-asked-questions. Also see Washington State Institutional Review Board Procedures Manual, Section 5.1 Determining if an activity requires WSIRB review and approval, pages 30 to 33, and the Washington State Agency Policy on Protection of Human Research Subjects. See https://www.dshs.wa.gov/sites/default/files/SESA/hrrs/documents/Procedures.pdf and https://www.dshs.wa.gov/sites/default/files/SESA/hrrs/documents/guideandpolicy.pdf.

- **Any entity when functioning as the lead organization** can request proprietary financial information, indirect patient identifiers, unique identifiers and other data, or any combination thereof, but not direct patient identifiers. Prior to the lead organization releasing any health data reports that use claims data, the lead organization must submit the reports to OFM for review. The lead organization also has to submit to OFM a list of reports it anticipates producing during the following calendar year.
- **Lead organization when not operating as the lead organization** can request indirect patient identifiers, unique identifiers and other data but not direct patient identifiers or proprietary financial information. The lead organization must follow the data release process.
- **Release upon request** includes claims or data that are limited to unique identifiers and other data only. The requesters do not need to follow the data release process or sign a confidentiality or data use agreement. An example of this release would be a public data set that could be downloaded from the APCD website.

For a data access summary, see Data Access under Chapter 43.371 RCW: Statewide Health Care Claims Data at http://www.ofm.wa.gov/healthcare/pricetransparency/pdf/data_access.pdf.

RCW 43.371.050(5) and (6) set the following parameters on the use of WA-APCD data in reports:

- The reports cannot contain proprietary financial information, direct patient identifiers, indirect patient identifiers, or any combination thereof.
- The reports can use geographic areas with a sufficient population size or aggregate gender, age, medical condition or other characteristics in the generation of reports as long as individuals are not identified.
- Reports that are issued by the lead organization at the request of providers, facilities, employers, health plans and other entities as approved by the lead organization can use proprietary financial information to calculate aggregate cost data for display in the reports. However, the lead organization must follow the format for the calculation and display of aggregate cost data adopted in rule to prevent the disclosure or determination of proprietary financial information.

RCW 43.371.060(5) states the office and the lead organization may not use claims data to recommend or incentivize direct contracting between providers and employers, but can use claims data to identify and make available information on payers, providers and facilities.

Chapter 43.371 RCW does not list a step-by-step process for data release. However, OFM noted that provisions in different sections of Chapter 43.371 RCW support the basic steps in the data release process used in other states. For purposes of discussion this section, OFM lists the basic steps in the data release process that are used in other states and the provisions in Chapter 43.371 RCW that support each step.

1. Data requesters submit a written data request to the lead organization.
   RCW 43.371.050(1) requires public and private data requesters to submit requests for processed data to the lead organization.

RCW 43.371.050(1)(a) to (h) lists the minimum information that must be included in the data request:

- The identity of any entities that will analyze the data in connection with the request;
- The stated purpose of the request and an explanation of how the request supports the WA-APCD goals to support transparent public reporting of health care information and improve transparency;
- A description of the proposed methodology;
- The specific variables requested and an explanation of how the data are necessary to achieve the stated purpose of the request;
- How the requester will ensure all requested data are handled in accordance with the privacy and confidentiality protections required in rule and any other applicable federal and state laws;
- The method by which the data will be stored, destroyed or returned to the lead organization at the conclusion of the data use agreement;
- How the protections will keep the data from being used for any purposes not authorized by the requester's approved application; and
- Consent to the penalties associated with the inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers or proprietary financial information.

2. **Review the data request.**
   RCW 43.371.020(5)(h) and (6) direct the lead organization to work with the data vendor to convene an advisory committee to provide advice on formal data release requests.[13]

3. **Approve or deny the data request.**
   RCW 43.371.050(2) authorizes the lead organization to decline a data request for the following reasons:
   - The data request does not include the information required.
   - The data request does not meet the criteria established by the lead organization's data release advisory committee.
   - For reasons established by rule.

4. **Release the data.**
   RCW 43.371.050(1) directs that the claims and other data from the database will be made available within a reasonable time after the request. The statute is silent on the length of time.

13. Per RCW 43.371.020(5)(h), the data release advisory committee members include in-state representation from key provider, hospital, public health, health maintenance organizations, large and small private purchasers, consumer organizations and the two largest carriers supplying claims data to the database.

RCW 43.371.50(7) requires that data recipients sign a DUA or confidentiality agreement prior to the data release. In the DUA, the data recipient must agree, at a minimum, to:

- Take steps to protect data containing direct patient identifiers, indirect patient identifiers, proprietary financial information, or any combination thereof, as described in the agreement.
- Not redisclose the claims data except if:
  - The claims data do not contain proprietary financial information, direct patient identifiers, indirect patient identifiers, or any combination thereof; and
  - The release is described and approved as part of the data request.
- Not attempt to determine the identity of any person whose information is included in the data set or use the claims or other data in any manner that identifies any individual or the individual's family or attempt to locate information associated with a specific individual.
- Destroy or return claims data to the lead organization at the conclusion of the data use agreement.
- Consent to the penalties associated with the inappropriate disclosures or uses of direct patient identifiers, indirect patient identifiers or proprietary financial information adopted in the APCD rules.

RCW 43.371.060(6)(b) directs the data vendor to have exclusive custody of the direct patient identifiers or proprietary financial information. The lead organization is not allowed to access this information. Accordingly, release of data extracts comes directly from the data vendor to the data requester. It does not go through the lead organization.

RCW 43.371.020(5)(f) directs that at the direction of the OFM, the lead organization and data vendor work to develop protocols and policies, including pre-release peer review by data suppliers, to ensure the quality of data releases and reports.

RCW 43.371.060(1)(a) directs the lead organization to submit the reports to OFM for review prior to releasing any health care data reports that use claims data.

RCW 43.371.060(3) directs the lead organization to not publish any data or health care data reports that:

- Directly or indirectly identify individual patients.
- Disclose a carrier's proprietary financial information.
- Compare performance in a report generated for the public that includes any provider in a practice with fewer than four providers.

RCW 43.371.060(4) directs the lead organization to not release a report that compares and identifies providers, hospitals or data suppliers unless:

- The data supplier, the hospital or the provider has an opportunity to verify the accuracy of the information submitted to the data vendor, comment on the reasonableness of conclusions reached, and submit to the lead organization and data vendor any corrections of errors with supporting evidence and comments within 30 days of receipt of the report.

- The lead organization corrects data found to be in error within a reasonable amount of time.
- The report otherwise complies with Chapter 43.371 RCW.

5. **Destroy or return data at the end of the project.**
   RCW 43.371.50(7)(d) requires that data recipients sign a DUA or confidentiality agreement prior to the data release. The data recipient must agree to destroy or return claims data to the lead organization at the conclusion of the data use agreement.

   The lead organization and data vendor have specific roles and responsibilities for the data release process that are designated in statute.

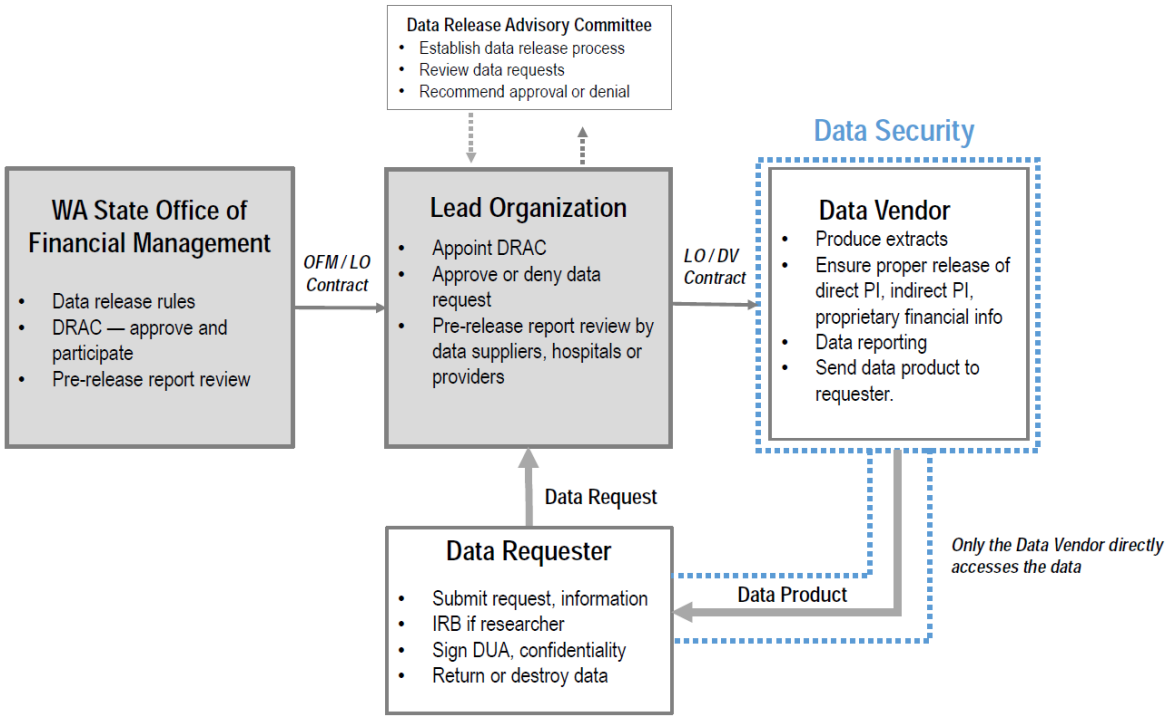
   RCW 43.371.020(5)(d)(f) and (h) direct the lead organization to:

   - Make information from the database available as a resource for public and private entities, including carriers, employers, providers, hospitals and purchasers of health care.
   - Develop protocols and policies, including pre-release peer review by data suppliers, to ensure the quality of data releases and reports.
   - Convene an advisory committee, with the approval and participation of the office, to establish a data release process consistent with the requirements of the law and provide advice on formal data release requests.

   RCW 43.371.020(3)(f) and (i) direct the data vendor to ensure that direct patient identifiers, indirect patient identifiers and proprietary financial information are released only in compliance with the terms of this chapter. The data vendor is also to maintain state-of-the-art security standards for transferring data to approved data requesters.

   Diagram A outlines the roles and responsibilities in Chapter 43.371 RCW for OFM, the lead organization, the data release advisory committee, the data vendor and the data requester in the WA-APCD data release process.

Diagram A: Chapter 43.371 RCW Roles and Responsibilities in the Data Release Process



E. PROVISIONS FOR PRIVACY AND SECURITY FOR WA-APCD DATA RELEASE

Chapter 43.371 RCW includes privacy and security provisions for data release.

RCW 43.371.050(1) directs that claims or other data from the database will be available only for retrieval in processed form to public and private requesters, except as otherwise directed by law. Only the data vendor has access to the claims and other data.

RCW 43.371.020(5)(c) directs the lead organization to work with the data vendor to ensure all patient-specific information is de-identified with an up-to-date industry standard encryption algorithm.

RCW 43.371.020(3)(e) directs the data vendor to assign unique identifiers to individuals represented in the database. This protects privacy yet allows identity matching.

RCW 43.371.020(3)(g) directs the data vendor to demonstrate internal controls and affiliations with separate organizations, as appropriate, to ensure safe data collection, security of the data with state of the art encryption methods, actuarial support and data review for accuracy and quality assurance.

RCW 43.371.020(3)(h) directs the data vendor to store data on secure servers that are compliant with the federal Health Insurance Portability and Accountability Act and regulations. Access to the data must be strictly controlled and limited to staff with appropriate training, clearance and background checks.

RCW 43.371.020(3)(i) directs the data vendor to maintain state-of-the-art security standards for transferring data to approved data requesters.

RCW 43.371.020(4) directs the lead organization and data vendor to submit detailed descriptions to the Office of the Chief Information Officer (OCIO) to ensure robust security methods are in place. The OCIO has policies that require the implementation of administrative, physical and technical safeguards to protect personal information that are no less rigorous than accepted industry practices, including the International Organization for Standardization's standards ISO-IEC 27002:2013 – Code of Practice for International Security Management, the Control Objectives for Information and related Technology (COBIT) standards and the current State of Washington Office of the Chief Information Officer IT Security Policy and Standards (OCIO 141.10).

RCW 43.371.020(2) requires OFM to use a competitive process to select a lead organization to coordinate and manage the database. In April 2016, OFM issued Competitive Procurement #16–100, which includes Appendix B Sample Contract to OFM CP #16-100. The sample contract contains provisions for confidentiality, privacy, security and audit in:

- Section 16. Protection of Confidential Information
- Section 17. Privacy Requirements
- Section 18. Security Requirements
- Sections 19. Contract Compliance – Audit by Third Party
- Section 20. Data Vendor Sight Audit Rights

See sample contract.

F. CONSIDERATIONS FOR PROCEDURES FOR DATA RELEASE AND PRIVACY AND SECURITY OF DATA RELEASE

Chapter 43.371 RCW includes detailed requirements for the data release process, data release documentation, and privacy and security for data release. The rules have to address procedures to fill the gap between what is required in law and what will be needed to administer the actual release of the WA-APCD data and ensure privacy and security.

OFM identified some of the considerations and questions from the research materials reviewed for this paper and listed them in the following sections.

Purpose of the data release
The statute lists the high-level purposes for the release of the WA-APCD data. Are specific guidelines needed in rule to evaluate data requests to determine if the request meets the statutory purpose?

Access to data
Only researchers with IRB approval can access identifiable data. Possible issues relating to the IRBs that researchers choose to review their projects include:

- Location of the IRB

    - In-state only. All researchers must use a Washington state-based IRB for their project review.
    - Out-of-state. Researchers can use IRBs located in other states. Should there be a requirement that the IRB be registered with the U.S. Department of Health and Human Services HHS?[14] Out-of-state IRBs have to comply with Washington state laws and policies related to protection of human subjects, which may be stricter than federal laws.
- Type of IRB
    - Public IRB
    - Private IRB
- Should the lead organization designate a specific IRB that all researchers requesting WA-APCD would use? This is what the Maryland APCD does.

The lead organization has to distinguish in advance to the office when it is operating in its capacity as a lead organization and when it is operating in its capacity as a private organization with respect to data access. Is a process that can be easily audited if needed to implement this provision?

Data release process

Is the basic data release process used by other states adequate for the WA-APCD? Should there be additional steps? Should steps be removed?

Are there aspects of the data release interaction between the lead organization and data vendor that should be in rule?

State agencies cannot pay fees for the data before it is released. When should nonstate data requesters pay the fees for the data?

- At the time the data request is submitted?
- After the data request is approved?
- Just prior to and as a condition for the data being actually released?

What type of proof do we want that the data have been destroyed?

Do we want timelines for some of the steps in the data release process? If so, which steps? Or do we want timelines for all of the steps in the data release process?

Data request

Only the minimum amount of data should be released to fulfill a data request.

The data request form has to include what is statutorily required. Should it contain the other items listed in Appendix C? If so, which ones?

Chapter 43.371 RCW authorized four levels of data access and six categories of data requesters. Should there be several data request forms that meet the statutory minimum requirements but are

14. The U.S. Department of Health and Human Services (HHS) regulations at 45 CFR part 46, subpart E, require all IRBs to register with HHS if they will review human subjects research conducted or supported by HHS. See IRB Registration Process Frequently Asked Questions at http://www.hhs.gov/ohrp/register-irbs-and-obtain-fwas/irb-registration/irb-registration-faq/index.html.

customized for the data requestor? This may be necessary to be administratively efficient for both the data requester and the lead organization.

Chapter 43.371 RCW is silent on publishing data requests. Other states publish data requests on their public websites so that all interested parties are aware of reporting/data uses.

- Should there be a public comment period on WA-APCD data requests? If so, how long?
- Should the public input occur before the data release advisory committee (DRAC) review? Public input becomes part of the DRAC review.
- Should the public input occur after the data request has been reviewed by the DRAC but before the lead organization authorizes the data vendor to release the data?
- How will the public input be used?
- Are there any provisions under Chapter 34.05 RCW Administrative Procedure Act that have to be considered if public input is part of the data request process?

The time to review data requests and release the data is affected by the complexity of the requests, availability of resources to fulfill the data request and the number of data requests. Should there be protocols for expedited review of data requests and release of approved data such as:

- Review data requests on a first-in first-out basis?
- Use information from previous requests to fulfill new requests if similar in nature and consistent with data release policies?
- Allow the lead organization to make "precedence"-based decisions on a data request without a formal DRAC review?

Data management plan

What should be included in the data management plan (DMP)?

Who should be involved in the technical evaluation of the DMP to ensure both the data and the state are protected?

If data recipients have changes in their data environments after the DUA is signed and the data released, how should these changes be handled? A revised DMP? New DUA? Should there be a timeline for reporting changes?

Does the data requester's DMP cover data management for subcontractors? Or does there need to be a DMP for each subcontractor as well as the data requester?

Data use agreement

If a data requester has a subcontractor, should the subcontractor sign an agreement with the lead organization and the data be transferred directly from the data vendor to the subcontractor?

Should the lead organization have a DUA with OFM when not operating as the lead organization?

Should there be a maximum length of time for a DUA? If so, how long?

- Can the data requester renew a DUA if the project is not complete? If so, for how long?
- If the data requester wants to use the same data for a different project, is a new DUA required? Can the current DUA be amended? Or should a new data request be required?

- DUA should contain a clause restricting release and use within the United States. How do we ensure that the data do not leave the country?
- DUA should contain the most if not all of the provisions listed in Appendix D.

Privacy and security

With respect to privacy and security for data release, OFM prepared a contract with the lead organization before the adoption of data release rule. Should the provisions for privacy and security provisions in the OFM/lead organization contract be included in rule?

Denial of data request

When a request is denied, should there be an appeal process? What should that process look like? Should it be the same or similar to review process already in rule?

Are there other considerations for data release or procedures for privacy and security to add to this list?

APPENDIX A: OTHER STATE DEFINITIONS RELATED TO DATA RELEASE

Appendix A lists definitions for data release terms used in the other state APCD rules.

Note that the list does not include the other state definitions for direct patient identifier, indirect patient identifier, proprietary financial information or unique identifier because RCW 43.371.010 defines these terms.

Term	Definitions related to data release
Analytic portal	*Colorado* "Analytic portal" means the APCD website www.cohealthdata.org and data access and analytical tools provided on behalf of Center for Improving Value in Health Care (CIVHC) in its role as APCD administrator by the APCD technology vendor.
APCD public user	*Colorado* "APCD public user" means any person accessing public facing reports and other information generated based on the APCD through the analytic portal developed and maintained on CIVHC's behalf by the APCD technology vendor.
Authorized user	*Colorado* "Authorized user" means an entity and the specific individuals named by that entity approved by CIVHC to access APCD data under the terms of a signed data use agreement.
Cell size	*New Hampshire* "Cell size" means the count of patients who share a set of characteristics contained in a statistical table *Vermont* "Cell size" means the count of persons that share a set of characteristics contained in a statistical table.
Data release application	*Colorado* "Data release application" means the application and supporting documentation an applicant or potential authorized user submits to CIVHC in its role as APCD administrator to request access to APCD data for a specified purpose.
Data release policies	*Colorado* "Data release policies" means the specific policies and procedures followed by the Data Release Review Committee in evaluating data release applications and in advising the APCD administrator.

Data set	*Oregon* "Data set" means a collection of individual data records whether in electronic or manual files. *Vermont* "Data set" means a collection of individual data records, whether in electronic or manual files.
Data release committee	*Colorado* "Data release review committee," as required under APCD rules, shall be appointed by the APCD administrator and is responsible for reviewing and making recommendations to the APCD administrator on the appropriateness of data release applications. *Maine* "Data release subcommittee" is a subcommittee of the Maine Health Data Organization (MHDO) board of directors established to review applications for data release as specified in these rules.
Data recipient	*New Hampshire* "Data recipient" is defined as the individual researcher, the organization or entity employing the researcher and the principal investigator. (This definition is found in the New Hampshire Limited Use Data Agreement.)
Data suppression	*Maine* "Data suppression" means the masking of certain data fields in situations where the small number of records in a subgroup might otherwise allow for the identification of individuals.
Data use agreement	*Colorado* "Data use agreement" means a document signed by CIVHC and an applicant that defines the terms and conditions under which access to and use of APCD data is permitted, as well as how the data will be secured and protected. *Maine* "MHDO data use agreement" is a MHDO document detailing a data recipient's commitment to data privacy and security, as well as restrictions on the disclosure and use of data.
De-identified data	*Colorado* "De-identified data set" has the meaning given to it by HIPAA, especially 45 CFR § 164.514(a). De-identification by the APCD will be achieved by removing all 18 identifiers enumerated at 45 CFR § 164.514(b)(2). *Maine* "De-identified data" means information that does not directly or indirectly identify an individual patient and for which there is no reasonable basis to believe the data can be used to identify an individual patient. MHDO Level I data are considered de-identified data. Level I data sets may be used only in ways that maintain patient anonymity and for acceptable MHDO uses.

De-identified health information	*Oregon* "De-identified health information" means health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual *Vermont* "De-identified health information" means information that does not identify an individual patient, member or enrollee and with respect to which no reasonable basis exists to believe that the information can be used to identify an individual patient, member or enrollee. De-identification means that health information is not individually identifiable and requires the removal of direct personal identifiers associated with patients, members or enrollees.
Disclosure	*New Hampshire* "Disclosure" means to communicate clinical or other health care information data collected pursuant to RSA 420-G: 11, II to a person not already in possession of the information. *Oregon* "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. *Vermont* "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
Encrypted	*New Hampshire* "Encrypted" means a method by which the true value of data has been disguised to prevent the identification of persons or groups and which does not provide the means for recovering the true value of the data.
Encrypted identifier	*Oregon* "Encrypted identifier" means a code or other means of identification to allow individual patients or enrolled members to be tracked across data sets without revealing their identity. *Vermont* "Encrypted identifier" is a code or other means of record identification to allow patients, members or enrollees to be tracked across the data set without revealing their identity. Encrypted identifiers are not direct identifiers.
Encryption	*Oregon* "Encryption" means a method by which the true value of data has been disguised to prevent the identification of individual patients or enrolled members and does not provide the means for recovering the true value of the data. *Vermont* "Encryption" means a method by which the true value of data has been disguised to prevent the identification of persons or groups and does not provide the means for recovering the true value of the data.

Health care claims data sets	*New Hampshire* "Health care claims data sets" means information consisting of or derived directly from member eligibility files, or medical, pharmacy or dental claims files submitted by health care claims processors collected under RSA 420-G:11, II and include public use data sets and limited use data sets.
Limited data set	*Colorado* "Limited data set" has the meaning given to it by HIPAA, especially 45 CFR § 164.514(e). *Maine* A "limited data set" includes limited identifiable patient information specified in HIPAA regulations. A limited data set may be disclosed to a data recipient without a patient's authorization in certain conditions: (1) the purpose of the disclosure must be limited to research, public health, health care operations; (2) the purpose of the disclosure must be consistent with the purposes of the MHDO; and (3) the data recipient must sign a MHDO DUA. The identifiable patient information that may remain in a limited data set for MHDO includes: A. dates such as admission, discharge, service, date of birth and date of death; B. city, state, five or more digit ZIP code, and C. age in years, months or days or hours. MHDO Level II data releases are a limited data set. Limited data sets may be used only in ways that maintain patient anonymity. *New Hampshire* "Limited use data set" means a health care claims data set that contains restricted data elements, which might be disclosed to an outside party for research purposes without the patient's authorization when (1) All direct patient identifiers have been encrypted in such a way as to not allow direct identification and to prevent linkage to other data sets where the patient can be directly identified; (2) Any data that directly identify or would lead to the indirect identification of health care practitioners performing abortions has been removed; and (3) All insured group or policy numbers cannot be used to directly identify a patient. *Oregon* "Limited data set" means protected health information that excludes direct personal identifiers and is disclosed for research or health care operations, or to a public health authority for public health purposes.
Longitudinal research	*Maine* "Longitudinal research" is a research method in which data are gathered for the same subjects repeatedly over a period of time. Longitudinal research projects can extend over years. Data recipients authorized to conduct longitudinal research may integrate the MHDO source data in their internal composite database for the purposes of internal longitudinal research.

MHDO assigned replacement number or code	*Maine* An "MHDO assigned replacement number or code" is a MHDO created number or code that is used to create anonymous or encrypted data indices. The MHDO assigned replacement number or code is not a direct identifier. MHDO assigned codes or numbers are owned by the MHDO and may be used only pursuant to MHDO DUAs and for no other purposes.
MHDO data	*Maine* "MHDO data" means all APCD data (health care claims data), hospital encounter data, hospital financial data, hospital baseline and restructuring data and quality data as defined in MHDO law. All information submitted to MHDO as required by law will be considered confidential data and protected by privacy and security measures consistent with health care industry standards.
Minimum necessary	*Maine* "Minimum necessary" is the principle requiring data applicants and recipients to make reasonable efforts to request and use only the minimum amount of data needed to accomplish the intended purpose of the data request for which MHDO approval was granted and for no other purpose.
Noncommercial redistribution	*Maine* "Noncommercial redistribution" is when an entity purchases MHDO data for inclusion in a larger composite database that is publicly released and available at no cost.
Principal investigator	"Principal investigator" is the person responsible for the data recipient's research project identified in the application and is responsible for the establishment and maintenance of security protocols to prevent authorized use or disclosure of data sets.
Protected health information	*Maine* "Protected health information" has the meaning given to it by HIPAA, especially 45 CFR §160.103, and will include written or electronic information relating to the diagnosis, treatment, tests, prognosis, admission, discharge, transfer, prescription, claims or other data or information implicitly or explicitly identifying a patient.
Public data	*Maine* "Public data" are data published on the MHDO publicly accessible website as required by Title 22, Chapter 1683. Public data include those parts of hospital financial data, described in Chapter 300, and quality data, described in Chapter 270, which are available on the MHDO publicly accessible website.
Public-facing reports	*Colorado* "Public facing reports" means reports and other information products generated based on the APCD database that provide aggregated, de-identified information that is available through the analytic portal.

Public use data set	*New Hampshire* "Public use data set" means a data set that is publicly available, contains data collected under RSA 420-G:11, II, is free of confidential data and from which all known direct or indirect patient identifiers have been removed in accordance with 45 CFR 164.514(a)-(b). *Oregon* "Public use data set" means a publicly available data set of de-identified health information containing only the data elements specified by the authority for inclusion. *Vermont* "Public use data set" means a publicly available data set containing only the public use data elements specified in this rule as unrestricted data elements in Appendix J.
Public health purposes	*Oregon* "Public health purposes" means the activities of a public health authority for the purpose of preventing or controlling disease, injury or disability including, but not limited to, the reporting of disease, injury, vital events such as birth or death and the conduct of public health surveillance, investigations and interventions.
Release	*New Hampshire* "Release" means to make all or part of the claims data set available for inspection and analysis to persons other than the department and the New Hampshire Insurance Department.
Research	*Maine* "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge, meaning knowledge that can be applied to populations outside of the population studied. *New Hampshire* "Research" means "research" as defined in 45 CFR 46.102(d). *Oregon* "Research" means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge.
Researchers	*Maine* Academic researchers, including those affiliated with public and private universities and medical schools, as well as other organizations and researchers undertaking health care research or health-care related projects.
Specialized report	*Colorado* "Specialized report" means any report or analytic data set generated based on the Colorado APCD that is not provided as a public-facing report available through the analytic portal.
Statistical table	*New Hampshire* "Statistical table" means single or multivariate counts based on the information contained in a data set and does not include any direct identifiers.

Strongly encrypted	*Oregon* "Strongly encrypted" means an encryption method that uses a cryptographic key with a large number of random keyboard characters.
Summarized data	*Oregon* "Summarized data" means data aggregated by one or more categories. Summarized data created from protected health information may not contain direct or indirect identifiers.
Supplemental data	*Maine* "Supplemental data" consist of data elements that are derived directly from the APCD data and the hospital encounter data. Specifically, supplemental data include the group ID elements and practitioner identifiable data elements as listed in Appendix C.

APPENDIX B: DATA ACCESS IN OTHER STATES

DATA ACCESS	CONTENT
Colorado	
Custom reports	"Custom report" means any report generated based on the APCD that is not provided as a public-facing report on the website. A custom report may provide summary-level statistics or analysis for subpopulations not otherwise available or identified in public-facing reports. A custom report does not display claims line or member-level detail.
De-identified data sets	Health information in which identifiers of the individual or relatives, employers or household members of the individual have been removed to meet the HIPAA standard of de-identification.
Limited data set	A limited data set contains some protected health information data elements but excludes a list of direct identifiers of the individual or of relatives, employers or household members of the individual.[15]
Identifiable information	Identifiable information refers to analytical data sets that include protected health information.
Maine	
Level 1 de-identified data	"De-identified data" means information that does not directly or indirectly identify an individual patient and for which there is no reasonable basis to believe the data can be used to identify an individual patient. MHDO Level I data are considered de-identified data. Level I data sets may be used only in ways that maintain patient anonymity and for acceptable MHDO uses.
Level 2 limited data set	A "limited data set" includes limited identifiable patient information specified in HIPAA regulations. A limited data set may be disclosed to a data recipient without a patient's authorization in certain conditions: (1) the purpose of the disclosure must be limited to research, public health, health care operations; (2) the purpose of the disclosure must be consistent with the purposes of the MHDO; and (3) the data recipient must sign a MHDO DUA. The identifiable patient information that may remain in a limited data set for MHDO includes dates such as admission, discharge, service, date of birth and date of death; city, state, five or more digit ZIP code; and age in years, months or days or hours. MHDO Level II data releases are a limited data set. Limited data sets may be used only in ways that maintain patient anonymity.

15. The direct identifiers are names; postal address information, other than town or city, state and ZIP code; Social Security numbers; medical record numbers; health plan beneficiary numbers; account numbers. The Colorado APCD does not collect telephone or fax numbers, email addresses, vehicle information, Web universal resource locators, Internet protocol address numbers.

Level III direct patient identifiers	"Direct patient identifiers" are personal information as outlined in Chapter 125, such as name, Social Security number and date of birth, that uniquely identifies an individual or that can be combined with other readily available information to uniquely identify an individual. An MHDO assigned replacement number or code (used to create anonymous data indices or linkage) is not a direct identifier. MHDO Level III data include direct patient identifiers.
Maryland	
Public use files	Includes data on facility or agency details, and patient demographics, cost and utilization. Also includes survey data available for long-term care facilities, home health agencies, hospices, ambulatory surgery centers.
Maryland medical care database	Includes research identifiable files and limited data sets for enrollment, provider and claims data for Maryland residents enrolled in private insurance, Medicare or Medicaid managed care organizations.
Washington, D.C. hospital discharge data	Includes research identifiable files and limited data sets for discharge abstracts for D.C. hospitals.
Massachusetts	
De-identified data	Providers, provider organizations, public and private health care payers, government agencies and authorities and researchers have access to de-identified data to study lowering total medical expenses, coordinating care, benchmarking, conducting quality analysis and other research, administrative or planning purposes.
Level 2	Level 2 data elements include limited patient-level information.
Level 3	Level 3 data elements include direct patient identifiers that may uniquely identify an individual.
New Hampshire	
Commercial claims public use data set	"Public use data set" means a data set that is publicly available; contains data collected under RSA 420-G:11, II; is free of confidential data; and from which all known direct or indirect patient identifiers have been removed in accordance with 45 CFR 164.514(a)-(b).
Commercial limited use data set	In accordance with 45 CFR 164.514(e)(3)(i), limited use data sets will be released only for purposes of research. "Research" means "research" as defined in 45 CFR 46.102(d).
Confidential health care claims research data set	"Confidential data" means individual or collective data elements contained in the claims data set that (1) have not been revealed previously to the public, and (2) directly identify a patient.

Oregon	
Summarized data	"Summarized data" means data aggregated by one or more categories. Summarized data created from protected health information may not contain direct or indirect identifiers
Public use data set	"Public use data set" means a publicly available data set of de-identified health information containing only the data elements specified by the authority for inclusion. The authority will maintain a list of data elements that may be included in APAC public use data sets. The public use data sets will comply with applicable authority policies and state and federal rules, regulations and statutes.
Limited use data set	"Limited data set" means protected health information that excludes direct personal identifiers and is disclosed for research or health care operations, or to a public health authority for public health purposes.
Identified data set	Contains direct identifiers and requires specific approvals such as patient consent. May be disclosed for purposes allowed by state and federal regulations, including research, public health and health care operations. "Research" means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge.
Vermont	
Classification of data elements	Unrestricted data elements: Data elements that are available for general use and public release as part of a public use file. Restricted data elements: Data elements that are not available for use and release outside the department except as part of a limited use research health care claims data set approved by the commissioner pursuant to the requirements of this regulation. Unavailable data elements: Data elements that are not designated as either unrestricted or restricted, or are designated as "unavailable." These data elements are not available for release or use outside the department in any data set or disclosed in publicly released reports in any circumstance.
Public use data sets	Unrestricted data elements collected or generated by the department or its designee that are made available in public use files and provided to any person upon written request, except where otherwise prohibited by law. The department maintains a public record of all requests for and releases of public use data sets.
Limited use health care claims research data sets	Limited use health care claims research data sets are those sets that contain restricted data elements, are not available to the public and are released to a requester only for the purpose of research upon a determination by the commissioner.

APPENDIX C: DATA REQUEST FORMS IN OTHER STATES

Data requesters complete, sign and submit data request forms to APCD administrators to request the release of data they need for their projects. The data requester provides the following information when completing a data request form:

- Purpose of the project and data request
- Research methodology
- Staff qualifications and résumés
- Funding source(s)
- Project timeline
- The analytic data set being requested, including data files and data elements
- The project's data management plan, including privacy and security provisions
- The techniques the data requesters will use to prevent re-identification of data when there are small numbers or subgroups. For example, Oregon's policy is data with small numbers (data where values are 30 or less ($n \leq 30$) or where subpopulations consist of 50 or fewer individuals ($n \leq 50$)) may not be disclosed in a way that can be used to re-identify an individual.
- APCD administrators require data requesters to comply with the APCD minimum cell suppression policies. For example, the Colorado APCD has a minimum cell size suppression policy that requires any cell in any report or data table, printed or electronic, with fewer than 11 records or observations to be replaced by "fewer than 11" or similar text. Data requesters must also apply complementary cell suppression techniques to ensure cells with fewer than 11 records cannot be identified by manipulating data in adjacent rows and columns.
- Information on any data linkages or combination with other data. The APCD administrator seeks to ensure that data cannot be re-identified if it is linked to or combined with information obtained from other sources. For example, the Colorado APCD requires justification for each proposed linkage of the requested data to other databases or proposed combination of the requested data with other data, including:
  - How the linkage or combination will contribute to achieving the project purpose
  - Whether the project can be completed without this linkage or combination
  - The steps to prevent the identification of individual patients
- Copies of current privacy and security policies from the data requester's organization
- Information on any third-party organization that may have access to the requested data. This information includes details about the staff who will be working with the data and copies of the third-party organization's current privacy and security policies.
- Contact information for the data requesters and third-party organizations involved in the project

Some states use one form for all data requests. Other states use several forms. Table 1 summarizes the data request forms by state.

Table 1: Data request forms in other states

State	Data Request Forms
Colorado	Has one data release application for all data requests.[16]
Maine	Has two data request summary forms: one to request restricted data and one to request unrestricted data.[17]
Maryland	Has three data request forms: a public use file form, a pre-application for research identifiable files and limited data sets from the APCD, and a main application. The pre-application provides the APCD staff with an overview of the research goals and includes an attestation that the applicant is aware of and able to comply with the data security standards. The main application details the project information, data management plans and data specifications.[18]
Massachusetts	Has two forms: a government agency request for APCD data that is used by U.S. federal agencies and departments and another for Massachusetts state agencies, departments and authorities. Data requests from other states, as well as other political subdivisions of Massachusetts, use the nongovernment agency request form.[19]
New Hampshire	Has two data request forms: one to request public use data sets and the other to request limited use data sets.[20]
Oregon	Has four data request forms:[21] ▪ APAC-2 is a pre-application form for APAC data files. All data requesters complete and submit this form. Staff review the pre-application forms and then send the data requesters one or more of the applications listed below: ♦ APAC-3 to apply for limited data sets ♦ APAC-4 to apply for public use data sets ♦ APAC-5 for a research application for limited data sets. This application is intended for researchers who belong to a covered entity.
Vermont	Provides public use data sets to any person upon written request except where prohibited by law. The APCD administrator maintains a public record of all requests for and releases of public use data sets. Has an application for limited use health care claims research data sets. Details of the application are listed in the rule. Studies using data sets for longer than two years may be subject to requirement to reapply.[22]

16. See Colorado's data release application http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwi8ma-9zebLAhUO9WMKHc2bCewQFggmMAI&url=http%3A%2F%2Fcivhc.org%2Fgetmedia%2Ff99fe405-e50a-4e4f-87b6-3fb684905b43%2FCO-APCD-Application-Streamlined-11_2015.doc.aspx%2F&usg=AFQjCNEZPGZhzAibHbSvsQ5zrmLH8FmJjQ.
17. See Maine's data request process https://mhdo.maine.gov/imhdo/data_rqst_process.htm. To see the data request summary forms click the hyperlink for "restricted" and "unrestricted."
18. See Maryland's data release http://mhcc.maryland.gov/mhcc/pages/apcd/apcd_data_release/apcd_data_release.aspx.
19. See Massachusetts government and nongovernment request forms http://www.chiamass.gov/application-documents.
20. See New Hampshire public use and limited data set forms https://nhchis.com/DataAndReport/DataSets.
21. See Oregon APAC data sets http://www.oregon.gov/oha/OHPR/RSCH/Pages/apac.aspx.
22. See Vermont Regulation H-2008-01, pages 15-16 http://www.dfr.vermont.gov/sites/default/files/REG-H-08-01.pdf.

APPENDIX D: DATA MANAGEMENT PLANS IN OTHER STATES

APCD administrators require data requesters to submit data management plans (DMP) with their data request forms. A DMP is a formal document that outlines how the data requester will handle the data both during the project and after the project is completed to ensure data privacy and security. In some states, provisions for the DMPs are included as part of the data request form.[23] In other states, the DMP is included as a separate document with the data request form.

The APCD administrators require data requesters to provide detailed information in their data management plans about the following:

1. **Physical possession and storage of the data files.** This includes details about the personnel handling the data; the facilities, hardware and software that will secure the data; and the physical, administrative and technical safeguards in place to ensure the privacy and security of the released data.
2. **Data sharing, electronic transmission and distribution.** This includes the data requester's policies and procedures for sharing, transmitting, distributing and tracking data files; physical removal and transport of data files; staff restriction to data access; and use of technical safeguards for data access (e.g., protocols for passwords, log-on/log-off, session time out and encryption for data in motion and at rest). It also includes information on additional organizations that may be involved in using the data as part of the project.
3. **Data reporting and publication.** This includes who will have the main responsibility for notifying the APCD administrator of any suspected incidents wherein the security and privacy of the released data may have been compromised; how DMPs are reviewed and approved by the data requester; whether the DMPs will be subjected to periodic updates during the DUA period for the released data; and an attestation that the data requester will adhere to the APCD's cell suppression policy of not publishing or presenting tables with cell sizes fewer than 10 or 11 (depending on the state) to anyone who is not an authorized user of the data.
4. **Completion of research tasks and data destruction.** This includes the data requester's process to complete the certificate of destruction form and the policies and procedures to:
    - Dispose of APCD data files upon completion of its research.
    - Protect the APCD data files when staff members of project teams (as well as collaborating organizations) terminate their participation in projects. This may include staff exit interviews and immediate termination of data access.
    - Inform the APCD administrator of project staffing changes, including when individual staff members' participation in research projects is terminated, voluntarily or involuntarily.
    - Ensure that the APCD data and any derivatives or parts thereof are not used following the completion of the project.

23. See the Colorado data release application, Part Three Data Management Plan at http://civhc.org/All-Payer-Claims-Database/Data-Release.aspx/.

The DMP may also have a section for assurances in which the data requester agrees to:

- Adhere to processes and procedures to prevent unauthorized access, disclosure or use of data, including the processes and procedures outlined in the DMP.
- Be subject to the requirements and restrictions contained in applicable state and federal laws protecting privacy and data security.
- Agree to establish and maintain appropriate administrative, technical and physical safeguards to protect the confidentiality of the data and prevent unauthorized use or access to it.[24]
- Notify the APCD administrator as soon as practicable of any unauthorized use or disclosure of data.
- Adhere to the DMP for the project and notify the APCD administrator of any material changes to the DMP during the project

Some states have separate DMP templates for different users. For example, Massachusetts has a separate DMP template that nongovernment data requesters use. Massachusetts also provides additional documents to help with the preparation and evaluation of a DMP.[25]

Some states list the minimum security requirements in the DMP that a data requester must meet to receive the APCD data. For example, the minimum security requirements for nongovernment applicants for data from the Massachusetts APCD are:

- Encryption of any media containing APCD data;
- Anti-virus software on any server containing APCD data; and
- Physical access controls, i.e., confidential data must be stored behind locked doors with access to the data limited to the fewest number of people required to achieve the purpose for which such access was granted.

Or

- An attestation by an organization's chief legal officer, or another attorney or officer authorized to bind an organization, that the organization complies with HIPAA privacy and security requirements or, if not a HIPAA-covered entity, has privacy and security practices and policies in place such that the organization is substantially compliant with HIPAA privacy and security rules.

24. Massachusetts requires a level and scope of security consistent with 45 CFR § 164.530(c) and not less than the level and scope of security requirements established by the Office of Management and Budget in OMB Circular No. A-130, Appendix III–Security of Federal Automated Information Systems http://www.whitehouse.gov/omb/circulars/a130/a130.html), as well as Federal Information Processing Standard 200 "Minimum Security Requirements for Federal Information and Information Systems" (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf) and Special Publication 800-53 "Recommended Security Controls for Federal Information" (http://csrc.nist.gov/ publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf).

25. In Massachusetts, documents for the nongovernment data management plan include the data management plan http://www.chiamass.gov/assets/Uploads/apcd-3-0/application-materials/Non-Government-APCD/5.-Data-Management-Plan-with-Mimimum-Security-Requirements.pdf; data management plan guidelines http://www.chiamass.gov/assets/Uploads/apcd-3-0/application-materials/Non-Government-APCD/DPSP-Data-Management-Plan-Guidelines.pdf; and data management plan evaluation and checklist http://www.chiamass.gov/assets/Uploads/apcd-3-0/application-materials/Non-Government-APCD/DMP-Review-Checklist-Evaluation-Guide.pdf.

Or

- Documentation sufficient to show that an organization's information security and privacy program has been subject to an independent third-party audit in the previous two years and the outside auditor determined that the organization is HIPAA-compliant.

APPENDIX E: DATA USE AGREEMENTS IN OTHER STATES

The data use agreement (DUA) is a legally binding document between the APCD administrator and the data recipient. The DUA defines the terms and conditions under which the state permits use of the APCD data, how the data will be secured and privacy protected, provisions in case of a breach and penalties for noncompliance.

DUA templates are usually included in the data request forms. The data requester submits a signed copy with the data request. Some states, such as Colorado, have one DUA for all data requests.[26] Other states have several DUAs. For example, Massachusetts has a DUA for government agencies and a DUA for nongovernment entities. Massachusetts also has an addendum to the DUA for government agencies receiving MassHealth data (Medicaid data) and an addendum to the DUA for recipients of Medicare data.[27] Oregon has a DUA for a public use data set and a more comprehensive DUA for research limited data sets.

The following list describes the provisions in other state DUAs. Some states have fewer provisions than those listed here.

- DUAs have beginning and ending dates. States allow data recipients to submit a written request for an extension if the data recipients' project requires a longer period of data use.
- DUA terms can be changed only by a written modification to the DUA or by the parties adopting a new agreement. For example, in Oregon, if a research project extends beyond one year from the beginning date of the DUA, the DUA must be reviewed and resubmitted.
- DUAs include information about the project and the data elements being requested. The data request is incorporated in the DUA as an attachment or exhibit.
- States retain all ownership rights to the data file(s) that are being released. The data recipients do not obtain any right, title or interest in any of the data furnished by the state APCD.
- Data can be used only for the purposes described in the request. The data recipient agrees not to use, disclose, market, release, show, sell, rent, lease, loan or otherwise grant access to the data files specified except as expressly permitted by the DUA or otherwise by law.
- With respect to analyses and displays of data, the data recipient agrees to:
  - Abide by the APCD cell suppression policy in the creation of any document (manuscript, table, chart, study, report, etc.). A cell suppression policy stipulates that no cell (e.g., admittances, discharges, patients, services, others) with fewer than a certain number of observations may be displayed — typically 11 observations in the state APCDs[28] and 10 observations for CMS data.
  - Use complementary cell suppression techniques in the preparation of reports and analytics to ensure that cells with fewer than 11 observations cannot be identified by manipulating data in adjacent rows or columns or other manipulations of the report.

26. For Colorado's data use agreement, see http://civhc.org/CIVHC-Initiatives/Health-Care-Delivery-Redesign.aspx/.
27. For Massachusetts data use agreements, see http://www.chiamass.gov/application-documents.
28. CMS cell size suppression policy is that no cell (e.g., admissions, discharges, patients, services) 10 or fewer may be displayed. Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell 10 or fewer. This applies to the creation of any document (manuscript, table, chart, study, report, etc.) concerning the purpose specified in the DUA.

Examples of such data elements include, but are not limited to, geographic location, age if > 89, sex, diagnosis and procedure, admission/discharge date(s) or date of death.
    - Not use percentages or other mathematical formulas if they result in the display of a cell displaying fewer than 11 observations.
    - Not publish individual-level records in any form, electronic or printed.
    - Link files only as described in the protocol approved by the APCD administrator. If these data are linked with other records or databases, use of the resulting linked database must comply with conditions of the DUA.
    - Not link data to other records or databases if the result allows for identifying individuals; taking legal, administrative or other actions against individuals; or contacting or assisting others to contact any patients and/or physicians who may be indirectly identified.
    - Not retransfer or redisseminate data in a format that could possibly lead to the identification of an individual.
    - To take full responsibility for the analysis of the data and communication of results.
- With respect to publishing reports, data recipients agree to:
    - Provide the APCD administrator with a preview copy of proposed reports or publications based in whole or part on the released data sets for review prior (15–20 days) to the publication or release.
    - Obtain approval from the APCD administrator to release any reports or outputs prior to distribution outside the named project team. Distribution includes, but is not limited to, peer review, submission to any federal or state agency, presentation of findings or synopsis of research.
    - When publishing or communicating results of their analysis, to provide a notation indicating that the APCD is not responsible for the analysis, conclusions and recommendations derived from the data sets, and that the requester or author does not represent the state.
- With respect to privacy and security of the data, the data recipients agree to:
    - Establish appropriate administrative, technical and physical safeguards to protect the confidentiality and prevent unauthorized use of or access to the data.
    - Not use unsecured telecommunications, including the Internet, to transmit individually identifiable or deducible information derived from the data sets.
    - Not physically move, transmit or disclose data in any way from or by the site indicated in the receiving organization's data management plan without written approval from the APCD administrator unless such movement, transmission or disclosure is required by law.
    - Maintain confidentiality of all information as to personal facts and circumstances obtained on individuals and not be divulged except as permitted by law and the DUA.
    - Comply with, and have their agents, contractors, subcontractors and employees comply with all applicable federal and state laws, rules and regulations applicable to the privacy, confidentiality or security of protected health information.
    - Grant access to its personnel, facilities and the data to the authorized representatives of the APCD administrator at the site indicated in the receiving organization's data management plan for the purpose of inspecting to confirm compliance with the terms of this agreement.
    - Destroy the data and provide proof of having done so within so many days of the end of the project. The grace period for data destruction is typically five to 60 days, depending

on the state. Most states require the completion and submission of a certificate of data destruction. See Appendix H: Timelines for the data release process in other states.

Data recipients must promptly notify the APCD administrator of any material institutional review board (IRB) actions involving the data provided under this agreement including, but not limited to:

- staff changes
- revision of the research protocol
- suspension or termination of approval of the research study
- research protocol violations
- noncompliance with IRB stipulations
- noncompliance with the DUA
- noncompliance with any policy, rule, regulation or statute governing the data recipient's research

- If a data recipient receives funding from a commercial entity, such as a pharmaceutical company or a health plan, the data recipient attests that the commercial entity has no editorial control over data recipient's publications regardless of the finding from data recipient's research and that data recipients will not disclose the data, nor any parts thereof, to any of the commercial entity's officers, agents, contractors, subcontractors or employees.
- The DUA must be reviewed and resubmitted no less than annually if the research project extends beyond one year from the date of this agreement. The ability of researchers to use the data under this agreement is valid for one year from the date of this agreement unless extended in writing.
- Use of the same data for a project other than the one described in the DUA must be approved through a separate application process. The data recipients understand and agree that original or derivative data file(s) cannot be reused or further disclosed without prior written approval from the APCD administrator.
- With respect to a breach of the DUA:
  - The data recipient agrees to report any unauthorized access, use, reuse or disclosure of the data promptly to the APCD administrator.
  - If APCD administrator is informed, or has a reasonable belief, that any unauthorized access, use, reuse or disclosure of the data have occurred, the APCD administrator may:
    - Investigate the matter, including on-site inspection for which the data recipient shall provide access.
    - Resolve the dispute by a plan of correction or other alternative.
    - Declare a breach of the DUA and demand the return of any and all data released under this agreement.
    - Provide no further data.
  - The APCD administrator may also exercise any and all legal, equitable and criminal referral remedies in the event of a breach of the agreement. In the event that the APCD administrator succeeds in a court action to invoke injunctive relief for a violation of the agreement, the data recipient pays reasonable attorney's fees and costs to the APCD administrator. The data recipient also agrees to indemnify and hold the APCD administrator harmless for any harm to third parties resulting from any breach by the data recipient of the DUA terms and to cooperate with the APCD administrator in its defense of any third-party claim involving the data recipient's activities under the DUA.

- Data recipients must require all agents, contractors, subcontractors or employees who receive or have access to the data to agree to the same restrictions and conditions on the use or disclosure of the data that apply to the data recipient.
- Either the APCD administrator or the data recipient can at any time and for any reason upon 30 days' notice may terminate the DUA.
- The obligations and limitations of the DUA extend beyond the termination or expiration of the DUA.
- Colorado is the one state that has an "antitrust compliance and indemnification provision" in its DUA that states:

"Receiving Organization agrees to treat APCD Data confidentially, as specified in this Agreement, and not to use, or enable any other parties to use, the APCD Data for anticompetitive or other unlawful purposes, including but not limited to price-fixing, market or customer allocation, service or output restriction, price stabilization, or any other agreement or coordination among parties that in any way restricts or limits competition. Receiving Organization also agrees to indemnify and hold Center for Improving Value in Health Care (CIVHC) harmless for any antitrust liability, damages, judgments, fees, expenses, awards, penalties (including civil monetary penalties), and costs (including reasonable attorneys' and court fees and expenses) arising from or relating in any way to the APCD Data, or that in any way involve use of the APCD Data. Such indemnification shall include, but not be limited to, payment by Receiving Organization of any fines, penalties, or damages of any sort, including but not limited to compensatory, treble, punitive, or any other damages, fines, or penalties assessed against CIVHC for any antitrust violation arising from or relating in any way or any part to the APCD Data or use of the APCD Data, as well any and all of CIVHC's related legal fees, costs, and/or other expenses incurred in or arising from the matter.

"Receiving Organization further agrees that it shall not attempt to identify parties that have been de-identified in the Reports, "reverse engineer," decompile, or in any other way attempt to discern the identities of the specific parties charging or paying any prices contained in the APCD Data, nor shall Receiving Organization try to translate, convert, adopt, alter, modify, enhance, add to, delete, or tamper with any APCD Data or in any other way attempt to calculate or determine specific parties' prices from the APCD Data."

APPENDIX F: CONFIDENTIALITY STATEMENT FOR MASSACHUSETTS NON-GOVERNMENT ENTITIES

CONFIDENTIALITY AGREEMENT

I, _____, hereby acknowledge that, in connection with a request for All-Payer Claims Database data and/or Hospital Discharge Database data under an agreement (the "Agreement") with CHIA, I may acquire or have access to confidential information or individually identifiable information of patients. This information includes, but is not limited to, patient level protected health information (PHI - eligibility, claims, providers), health insurance coverage information, financial institution match information, as well as "personal data" as defined in G.L. c. 66A (collectively, the "Information").

I will comply with all of the terms of the Agreement with CHIA regarding the access, use, and disclosure of any Information provided by CHIA.

I will at all times maintain the confidentiality of the Information. I will not inspect or "browse" the Information for any purpose not outlined in the Agreement. I will not access, or attempt to access, my own Information for any purpose. I will not access, or attempt to access, Information relating to any individual or entity with which I have a personal or financial relationship, for any reason. This includes family members, neighbors, relatives, friends, ex-spouses, their employers, or anyone not necessary for the work assigned. I will not, either directly or indirectly, disclose or otherwise make the Information available to any unauthorized person at any time.

I understand that any violations of this Agreement, M.G.L. c. 93H (regarding data breaches), M.G.L. c. 93I (regarding data destruction), and other laws protecting privacy and data security may subject me to criminal or civil liability. I further understand that CHIA will notify state and federal law enforcement officials, as applicable, of any data breaches in connection with any violation of this Agreement.

Signed: _____

Signature Date: _____

Print Name: _____

Title: _____

Organization: _____

Address: _____

Telephone: _____ E-Mail:_____

APPENDIX G: COLORADO'S CERTIFICATE OF PROJECT COMPLETION AND DATA DESTRUCTION OR RETENTION

CIVHC
CENTER FOR IMPROVING VALUE IN HEALTH CARE

APPENDIX I
CERTIFICATION OF PROJECT COMPLETION AND DESTRUCTION OR RETENTION OF DATA (PLEASE SAVE)

Name:	
Title:	
Organization:	
Address:	
Tel Number:	
Fax Number:	
E-mail Address;	
Project Title:	
Data Sets:	
Years:	
❒ Certification of Data Destruction Date the Data was Destroyed:	
❒ Request to Retain Data	Date Until Data Will Be Retained:

Instructions: Data must be destroyed so that it cannot be recovered from electronic storage media in accordance with the methods established by the "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," as established by the U.S. Department of Health and Human Services (HHS).
I hereby certify that the project described in the Application is complete as of this date _____, ___, 20__.

Complete the appropriate section, below:

❒ I/we certify that we have destroyed all Data received from the CO APCD Administrator in connection with this project, in all media that were used during the research project. This includes, but is not limited to data maintained on hard drive(s), diskettes, CDs, etc.

❒I/we certify that we are retaining the data received in connection with the aforementioned project, pursuant to the following health or research justification (provide detail, use as much additional space as necessary and state how long the data will be retained).

❒ I/we hereby certify that we are retaining the Data received from the APCD Administrator in connection with the aforementioned project, as required by the following law. [Reference the appropriate law and indicate the timeframe].

APPENDIX H: TIMELINES FOR THE DATA RELEASE PROCESS IN OTHER STATES

These timelines are found in state APCD rules, policies, or data use agreements.

Date Release Process	Timelines for Data Release
Submit data request	*Colorado* Applications must be submitted at least 15 days prior to a regularly scheduled data review committee meeting to be considered at that meeting.
Review data request	*Colorado* The APCD administrator conducts reviews of the applications for completeness. If the application is incomplete, the APCD administrator may require supplemental information and must notify the applicant of its decision within 45 days of receipt of such information. The APCD administrator will provide access to applications and related materials at least 10 days prior to DRRC meetings via the secure DRRC website. *Oregon* If the data request application is incomplete, the requester has 30 calendar days from notification of incompleteness to complete the application. Incomplete applications that are not completed are discarded without further notification to the requester. If the DRC requests clarification, the requester has 30 calendar days to provide the requested information. After 30 calendar days, applications with incomplete requests for clarification are discarded without further notification to the requester. *Maine* The APCD administrator convenes the data release subcommittee no later than 60 business days after the initial posting of the data request on the MHDO website to review and consider Level III applications. The APCD administrator posts the data requests on the website and allows 30 days for data suppliers and other interested parties to provide input on the data request. *Vermont* The claims data release advisory committee provides the commissioner with any comment on the merits of the research application within 30 days.
Approve or deny the data request	*Colorado* A summary of each approved application will be posted on the data release section of the CIVHC website unless a specific embargo period is negotiated with the administrator. Unless otherwise negotiated or agreed to, application summary information will be posted within six months of DRRC approval. *Oregon* The APCD administrator has to approve or deny the completed request and provide written notification to the requester within 30 calendar days of receipt of the request. *Vermont* If the commissioner declines to release the requested limited use data sets

Date Release Process	Timelines for Data Release
	within 60 days of receipt of a complete application, the department will give written notice of the basis for denial of the application and the requester has leave to resubmit or supplement the application to address the commissioner's concerns.
Release data	*Maine* The APCD administrator must release the data no fewer than 10 days after the electronic notification of the data release approval is provided and the data requester meets the requirements of the rules. The data will be released as approved unless a data provider or data applicant takes action within 10 business days of the electronic notification by submitting in writing to the attention of the APCD administrator a request for review to the next higher authority. The request should clearly state the basis for the review or requested action. *Vermont* If the commissioner declines to release the requested limited use data sets within 60 days of receipt of a complete application, the department will give written notice of the basis for denial of the application and the requester has leave to resubmit or supplement the application to address the commissioner's concerns.
Submit proof of data destruction or retention	*Colorado* The receiving organization agrees to notify the APCD administrator within 30 days of the completion of the project purpose (as specified in section I of the application) if the project is completed before the last day of the data retention period (as specified in the project schedule). When retention of the data is no longer justified and/or required by law, the receiving organization agrees to destroy the data and send a completed "Certification of Project Completion & Destruction or Retention of Data" form (Appendix 1 to this agreement) to the APCD administrator within 30 days. *Maine* The written certification to verify the destruction or return of data must be submitted within five days of the completion of the stated purpose of the data use or demand. *Massachusetts* Return or destroy data or derivative data within 30 days of (1) completion of the research described in the application; (2) termination for any reason of the data recipient's DUA; (3) termination of DUA. Within five days of the completion of any requested destruction, the data recipient shall provide CHIA with a written certification that destruction has been completed in accordance with the required standards and that the data recipient and its contractors and agents no longer retain such data or copies of such data. DUA for non-government entities Recipient notifies CHIA within 30 days of the completion of the purposes specified in the DUA if completed before retention date. Upon this notice or retention date, whichever occurs sooner, the recipient agrees to destroy the data and send written certification of the destruction of the files to CHIA within 30 days of the retention date, using the form titled Certificate of Project Completion and Data Destruction.

Date Release Process	Timelines for Data Release
	New Hampshire Effect of termination. Upon termination or expiration of this agreement for any reason, data recipient will within 30 days return all data sets and provide written certification of the return and/or destruction of all data sets and copies of data sets. *Oregon* Data will be destroyed and an attestation provided to that effect or the data will be returned not later than 60 days after completion of the research project. An investigator will notify Oregon Health Authority within 30 days of the date of completion of the research project if completed before the specified completion date. Investigators will submit confirmation that no copy, data, nor parts thereof have been retained, and that the data have been destroyed or have been returned *Vermont* Within 30 days after the scheduled completion date of the project, the requester must either: ▪ Delete, destroy or otherwise render the data unreadable, so certifying by submitting a written notice to the department, or ▪ Reapply for approval if the end date of the project needs to be extended.
Review of report or products containing released data by APCD administrator prior to release of report or products	*Colorado* The receiving organization agrees to provide the APCD administrator with a copy of any results derived from the APCD data and information on the outcome of the project, as described in the application. The APCD administrator will review the report within six weeks of receipt. *Maine* Data recipients must provide the report or product that uses the released data at least 20 business days prior to the release of the document. *New Hampshire* Provide department with a preview copy of proposed reports or publications based in whole or part on the data sets at least 15 days prior to the publication or release. *Vermont* Data recipients must provide a copy of any proposed report or publication containing information derived from the data at least 15 days prior to any publication or release.
Extension of data use agreement	*Maryland* Two-year retention: The terms of this agreement are valid for two years from the date of signing, and additional time for data use will require the requester to submit a new IRB application. Upon expiration of this agreement, the requester must provide verification that the data has been destroyed. *New Hampshire* If data recipient determines that its research project needs to be extended, data recipient shall submit a written request to department at least 60 days before the expiration date. *Oregon* The data use agreement must be reviewed and resubmitted no less than annually if the research project extends beyond one year from the date of this agreement. The

Date Release Process	Timelines for Data Release
	ability of investigators to use the data under this agreement is valid for one year from the date of this agreement unless extended in writing.
Termination of DUA	*Colorado* The APCD administrator or the receiving organization may terminate this agreement at any time for any reason upon 30 days written notice. *New Hampshire* Upon termination or expiration of this agreement for any reason, data recipient shall within 30 days return all data sets and shall provide written certification of the return and/or destruction of all data sets and copies of data sets.
Appeal	*Oregon* A data requester can appeal a denied data request within 30 business days of the denial. *Vermont* Any adverse decision on an application may be appealed within 30 days by filing a request for hearing with the commissioner.

REFERENCES FOR DATA RELEASE

1. Colorado: http://civhc.org/All-Payer-Claims-Database/Data-Release.aspx/
2. Maine: https://mhdo.maine.gov/imhdo/rules.htm See Chapter 120 provisionally adopted rule March 2016.
3. Maryland: http://mhcc.maryland.gov/mhcc/pages/apcd/apcd_mcdb/apcd_mcdb.aspx
4. Massachusetts: http://chiamass.gov/assets/docs/g/chia-regs/957-8.pdf
5. New Hampshire: http://www.gencourt.state.nh.us/rules/state_agencies/he-w900.html
6. Oregon: http://www.oregon.gov/oha/OHPR/RSCH/Pages/apac.aspx
7. Vermont: http://www.dfr.vermont.gov/sites/default/files/REG-H-08-01.pdf
8. Washington Health Alliance All-Payer Claims Database Data Release Advisory Committee Summary of Recommendations. Available on the OFM Price Transparency Website at http://www.ofm.wa.gov/healthcare/pricetransparency/.